U.S. Department of the Interior

Interior Enterprise Architecture

TRM Guidance Volume 2

TRM Architectural Principles

DRAFT

June 24, 2005

1 Application Integration/Interoperability

1.1 Application Development

Systems must be designed, acquired, developed, or enhanced such that data and processes can be effectively shared, for appropriate purposes, across Interior and with our partners.

Rationale

Ensures more consistent information by reducing multiple sources of data.

Better serves our customers (e.g., the public, employees, etc.) through increased

Reduces costs by eliminating duplicate systems or processes.

Supports better decision-making and accountability through shared data and processes.

Implications

Design systems that allow future repartitioning to avoid difficult data management, inefficient processes and to mirror changing business processes.

Research and acquire new tools that enable data sharing and provide training for their proper use.

Plan for modularity in application functionality and design.

Design for platform independence.

Consider enterprise wide impacts when designing enhancing, acquiring COTS/GOTS or extending the scope or use of applications.

Utilize a methodology to determine the appropriate balance between data and process integration and interoperability.

2 Basic Services

2.1 Infrastructure

A basic set of information services will be provided to all employees.

Rationale

Potentially reduces total cost (TCO) of ownership.

Provides basis for improved communication.

Consistent IT capability provides the basis for larger business initiatives and greater access to information.

Implications

Basic network connectivity for voice, internet, etc. needs definition (e.g., least common denominator).

Support requirements for basic services will increase (e.g., “I can’t get to the internet, why?”- help desk).

May require 24x7 operation and associated personnel availability and costs.

Need clarification of who will pay and how for increasing basic services (e.g., new

More training will need to be provided to the entire organization for any addition to or modification of the basic services.

For places where basic services cannot be provided, alternate processes/ methods need to be created (e.g., wildlife refuge 300 baud connection).

May increase initial costs for deploying personnel.

Network bandwidth will increase significantly as set of “basics” increases.

3 Business Re-engineering

3.1 Records Mgmt

Business process reengineering projects will explicitly incorporate records management requirements.

Rationale

Work processes, activities, and associated business rules will be well understood and documented.

Ensures that records are managed and protected appropriately.

4 Compliance

4.1 Records Mgmt

Records/document management solutions will comply with the Department of Defense (DOD) 5015.2-STD. (Design Criteria Standard for Electronic Records Management Software Applications- November 1997).

Rationale

Enables greater use of commercial-off-the-shelf solutions.

Complies with National Archives and Records Administration (NARA).

Avoids dependence on weak vendors.

5 Computer Security Incident Response Capability (CSIRC)

5.1 Security

Interior will coordinate an incident response capability that will be shared across all bureaus.

Rationale

Reduces risk, improves recovery time and/or minimizes damage.

Establishes the linkages between policy enforcement and system monitoring.

Required by federal laws and regulations.

Builds knowledge base, which allows security to be proactive through information sharing of alerts and vulnerability notifications.

Supports the generally accepted principles and practices of IT security.

Implications

Need criteria to determine when incidents come under “fraud, waste and abuse” that requires further action (e.g., law enforcement).

Need to develop criteria for incident response procedures.

Need for staffing with knowledgeable people.

Need IT security communication system tied into incident response capability.

Need to develop knowledge base repository.

Need to develop a “trusted” information sharing system for CSIRC among bureaus, to which only certain trusted people will have access.

Need to acquire supporting tools and training.

Need to develop consistent, documented CSIRC procedures across Interior.

Need to develop law enforcement linkages

Need 24 x 7 capability for security (e.g., alert notifications).

6 Continuity of Operations Planning

6.1 Infrastructure

An assessment of business continuation and recovery requirements is mandatory when acquiring, developing, enhancing or outsourcing systems. Based on that assessment, appropriate disaster recovery and business continuity planning, design, testing and

Rationale

Customers and partners have heightened awareness of the need for systems

Any significant visible loss of system availability and stability could negatively impact our mission and legal responsibilities.

Application systems and data are valuable organization assets that must be protected.

Implications

Operation and systems plans will need to be categorized according to business recovery needs (e.g., short term essential and long term essential).

Plans for work site recovery will need to be in place.

Continuity of Operations Planning (COOP)/ Continuity of Business Operations (COBO) will require periodic testing and revision.

Life cycle and other costs will increase.

Systems should be designed with appropriate level of fault tolerance and recovery in

6.2 Security

Appropriate disaster recovery and business continuity planning, design, testing and maintenance must take place. System Contingency plans are an integral part of these planning

Rationale

Application systems and data are valuable organization assets that must be protected.

Any significant visible loss of system availability and stability could negatively impact our mission and legal responsibilities.

Customers and partners have heightened awareness of the need for systems

Required by federal laws and regulations

Implications

Disaster Recovery Plans (DRPs) and Business Recovery Plans (BRPs) will require periodic testing and revision.

Plans for records recovery and alternate data capture mechanisms/processes need to be in place.

Operation and systems plans will need to be categorized according to business recovery needs (e.g., short term essential and long term essential).

Plans for work site recovery will need to be in place (e.g., office space).

Systems should be designed with appropriate level of fault tolerance and recovery in

Alternate information processing capabilities need to be in place.

Life cycle and other costs may increase.

Business impact analysis needs to be conducted in the first phase of life cycle process (e.g., an assessment of business continuation and recovery requirements will be mandatory when acquiring, developing, enhancing or outsourcing systems).

7 Continuity of Operations Planning (COOP

7.1 Records Mgmt

An assessment of business continuation and recovery requirements is mandatory when acquiring, developing, enhancing or outsourcing systems. Based on that assessment, appropriate disaster recovery and business continuity planning, design, testing and

Rationale

Any significant visible loss of system availability and stability could negatively impact our mission and legal responsibilities.

Application systems and data are valuable organization assets that must be protected.

Customers and partners have heightened awareness of the need for systems

8 Data and Information Stewardship

8.1 Application Development

Data and information must be managed and maintained as a stewardship responsibility to support the mission of Interior.

Rationale

Without stewardship, data can lose its value.

Stewardship program will support common business rules, which would facilitate information sharing and improve data integrity.

Data is a resource important to the accomplishment of Interior's work. In its broadest sense, it is information including items like electronic and paper records, emails, film, etc. Like natural resources, information needs stewards who are responsible for its valuation, preservation, security, access and utilization across Interior and with the

Without stewardship, information may cause confusion and result in harm to the department (e.g., litigation.)

Since information is an asset, it needs to be actively managed which is the goal of a stewardship program.

Implications

Understanding of customer needs for the information;

Need to develop a data stewardship program that will transcend many organizational boundaries (e.g., no current rewards for cross-bureau cooperation) and include various levels of stewardship while leveraging and adhering to Federal data programs and standards (e.g., FGDC, NIST).

Need for clarity around the role of the public as co-holders of responsibility around stewardship of their information.

Need to recognize that the "visual identity" or "branding" of the Interior-wide Web experience itself is an information asset.

Recognition of the need to manage "meta" data; that is data "about" the data.

Sensitivity to the sources and uses of the information, ensuring security, confidentiality and privacy are protected.

Need to recognize that stewardship includes things like:

Responsibility for clarification of the data's meaning, content, and reuse;

Understanding the entire "life cycle" of the data (e.g., currency, obsolescence;)

Responsibility and accountability for managing data's consistency, timeliness, accuracy and completeness;

Recognition that some information/data held by Interior but supplied by 3rd parties may need to be maintained/archived even if the originating organization disappears (e.g., oil lease information).

Recognition that business area personnel need to be responsible for stewardship of the data (with the support of IT) and the commitment of the resources necessary to make stewardship happen.

8.2 GIS

Data and information must be managed and maintained as a stewardship responsibility to support the mission of Interior.

Rationale

Data stewards will promote common business rules, which would facilitate sharing information, communication, and improved data integrity.

Supports Office of Management and Budget (OMB) Circulars: A16 "Coordination of Surveying, Mapping and Related Spatial Data Activities"; A-119 "Federal Participation in

the Development and Use of Voluntary Standards"; and A-130 "Management of Federal

Data is a resource important to the accomplishment of Interior's work. In its broadest sense, it is information including items like electronic and paper documents (e.g., maps), emails, film, etc. Like natural resources, data needs stewards who are responsible for its valuation, preservation, security, access and utilization across Interior and with the

Supports Executive Order 12906 "Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure".

Implications

Responsibility of steward for training and education in a persistent and consistent manner (e.g., software, data, and methodology changes regularly).

Need to develop a data stewardship program that will transcend many organizational boundaries (e.g., no current rewards for cross-bureau cooperation) and include various levels of stewardship while leveraging and adhering to Federal data programs and standards (e.g., Federal Geographic Data Committee (FGDC), National Institute of Standards and Technology (NIST)).

Recognition of the need to manage metadata; that is data "about" the data.

The scope of stewardship must be very sensitive to the sources and uses of the information, ensuring security, confidentiality and privacy are protected.

Recognition that business area personnel need to be responsible for stewardship of the data and the commitment of the resources necessary to make stewardship happen.

Stewardship includes responsibility for clarification of the data's meaning, content, and

Stewardship includes responsibility for managing data's consistency, timeliness, accuracy and completeness.

8.3 Records Mgmt

Data and information must be managed and maintained as a stewardship responsibility to support the mission of the department.

Rationale

Data stewards will promote common business rules, which would facilitate information sharing and improve data integrity.

Data is a resource important to the accomplishment of Interior's work. In its broadest sense, it is information including items like electronic and paper records, emails, film, etc. Like natural resources, data needs stewards who are responsible for its valuation, preservation, security, access and utilization across Interior and with the public.

8.4 Security

Protection of the data and information must be managed and maintained as a stewardship responsibility to support the mission of the department.

Rationale

Data stewards will promote common business rules, which will facilitate information sharing and improve data integrity.

Data needs stewards who are responsible for its valuation, preservation, integrity, security, access and utilization across Interior and with the public.

Implications

A clear process to assign and document stewardship responsibility on a application/system basis needs to be established and published.

Recognition that business area personnel need to be responsible for stewardship of the data and the commitment of the resources necessary to provide an adequate level of

There must be support for adhering to federal laws, executive direction, guidelines and the generally accepted principles and practices of IT security.

Stewardship includes responsibility for managing data's consistency, timeliness, accuracy completeness, and the necessary security training and awareness.

The scope of stewardship must be very sensitive to the sources and uses of the information, ensuring that confidentiality and privacy are protected (e.g., manage & accept risk and accreditation).

Metadata will need to include a security classification or identification.

Criteria used for classifying information/data needs to be flexible to accommodate changes in the threat environment (e.g., Homeland security).

9 Data Collection and Reuse

9.1 Data Management

In considering data requirements, we should look to reuse existing data before we buy. If no data exists within Interior, consider acquisition of data from external sources before collecting/creating new data.

Rationale

Supports the Federal Activities Inventory Reform Act, Paperwork Reduction Act and Clinger-Cohen Act.

Saves time.

Leads to increased data quality and integrity.

Saves money.

Supports the promotion of standards.

Implications

Data that is common among many business applications will be sourced and updated from a single authoritative source.

Need a clearinghouse of metadata for existing data.

If you are going to acquire data, consider facilitating its use by all of Interior.

We are at the “supplier’s” mercy for future cost, quality, availability, service and

Potential data sources’ data quality must be validated before acquisition or collection of

Need a standard process for acquiring data, when formal agreements are required.

When acquiring data from private vendors, licensing restrictions should be considered.

Good data requirements are needed to evaluate potential data sources.

10 Data Contingency Planning

10.1 Data Management

Contingency planning processes need to be in place to ensure data availability.

Rationale

Complies with Federal Preparedness Circular 65, FEDERAL EXECUTIVE BRANCH CONTINUITY OF OPERATIONS (COOP).

Allows Interior to continue its mission and meet legal requirements.

Ensures continued operations.

Supports Interior Continuity of Operations (COO) plans.

Protects Interior data.

Implications

Alternative off-site data archives need to be in place and synchronized.

Resources must be provided for data recovery testing.

Need to establish data recovery priorities.

Need periodic reassessment of bureau/Interior COO plans to ensure data availability is addressed.

11 Data Lifecycle

11.1 Data Management

Information is valued as an Interior asset; therefore, Interior data needs to be managed throughout its lifecycle.

Rationale

Data has its own lifecycle related to the lifecycle of the mission, not the information

Promotes the wise use of Interior data assets._

Meets the legal requirements of Paperwork Reduction Act, Government Paperwork Elimination Act, Federal Records Act, Clinger-Cohen Act, the OMB Information Initiative on the National Spatial Data Infrastructure and OMB Circular A-130 regarding data quality (i.e., utility, objectivity and integrity).

Managed data improves the ability to accelerate sound decision-making.

Increases the usefulness and value of data.

Facilitates data reuse and locating data at each stage of its lifecycle (including

Implications

Need a consistent data management process.

Data management (including its on going storage and archiving) is a mission cost that transcends an individual project.

Need ongoing management support and oversight throughout the data lifecycle: data stewards, data managers and data administrators.

Integrate data resource planning with business and information technology planning.

Interior needs to dedicate resources to data management in addition to relying on the DBA function.

Data quality is everyone's responsibility.

Management of data needs to be tied to workflow of the business process.

12 Data Security

12.1 Data Management

Data needs to be secured according to its sensitivity.

Rationale

Helps safeguard confidential and proprietary information.

Enhances public trust.

Complies with the Computer Security Act, the Privacy Act, the Government Information Security Reform Act, Office of Management and Budget (OMB) Circular A-130 Appendix 3, Electronic Freedom of Information Act Amendments of 1996, Computer Matching and Privacy Protection Act and Section 515 of the Treasury and Consolidated

Enhances the proper stewardship over information.

Helps to ensure legal and proper use of information.

Enhances the integrity of the information.

Implications

Need to conduct periodic (re)assessments of data classifications.

May need to edit sensitive data that is released to the public.

Data stewards will require training on this "new" stewardship responsibility.

May require additional resources (e.g., personnel, hardware and software).

Need to establish data sensitivity and privacy classifications and a review process.

Will lead to the use of authentication technologies; for example, digital signatures or passwords.

Employees and contractors will require training regarding use of sensitive data.

13 Data Sharing

13.1 Data Management

Data and information must be managed to facilitate data sharing across Interior, with our partners and the public.

Rationale

Achieves economies of scale, especially through cooperative data collection efforts.

Reduces duplication of effort.

Enhances reusability of data and information.

Leads to increased data quality.

Conforms with the Government Paperwork Elimination Act, Clinger-Cohen Act, Paperwork Reduction Act, Electronic Freedom of Information Act Amendments of 1996 and section 508 of the Rehabilitation Act.

Implications

Need to establish common core data standards, including data definitions.

Sharing and access needs to be timely.

Data should be made available in a variety of formats suitable for the user.

Need to agree upon and establish a common data standards process.

Need to agree upon data exchange mechanisms and protocols.

Need a consistent data management process.

Data that is common among many business applications will be sourced and updated from a single authoritative source.

Data and information resources will need to be defined in bureau and department information architectures.

The value of information is increased when not held in isolated pockets.

Need to take electronic records management requirements into consideration.

Need to balance the desire to share data with sensitivity, privacy and confidentiality

Additional effort may be required in the presentation of data to meet accessibility

Need well-documented and defined metadata.

14 Data Standards

14.1 Data Management

Interior will strive to create, acquire, and share data that adheres to data standards defined internally, with consideration to existing national standards.

Rationale

Facilitates the migration of data.

Using existing national standards reduces burden on Interior and complies with OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.

Facilitates exchange of data.

Makes data collection more consistent and increases data quality, compatibility, integrity.

Implications

Data stewards will identify and manage data standards model to be effective.

Need the ability to review the data standards and determine appropriateness.

Interior needs to increase participation in standards organizations to make it more likely to get industry adoption of standards that serve Interior's needs.

Long-term commitment of resources will be needed to establish and maintain data

Need to raise awareness of applicable standards.

Adopting standards may require changes to existing data or planning for migration to the new standard.

Need to develop a data standards program that will transcend many organizational

Need to establish common data standards, including data definitions.

15 Data Stewardship

15.1 Data Management

Data and information must be managed and maintained as a stewardship responsibility to support the mission of the department.

Rationale

Complies with requirements of Section 515 of the Treasury and Consolidated Agency Appropriation Act.

Data stewardship promotes the establishment of authoritative sources.

Data stewardship promotes common business rules, facilitates information sharing and improves data integrity.

Data is a resource critical to the mission of Interior. Like natural and cultural resources, data needs stewards who are responsible for its valuation, preservation, security, access, quality, and utilization.

Implications

Need to include various levels of stewardship while leveraging and adhering to Federal data programs and standards (e.g., Federal Geographic Data Committee (FGDC), National Institute of Standards and Technology).

Data stewards need to ensure that metadata is captured and managed.

Need to develop a data stewardship program that will transcend many organizational boundaries. Need to define data stewardship responsibilities that span the entire data

Need to identify and train subject matter experts as data stewards.

16 Design for Meaningful Data

16.1 Application Development

Applications must be designed to create, store, access and present data meaningfully.

Rationale

Increased access leads to improved integrity and relevance of data

Leads to greater data consistency.

Reduces unnecessary data redundancy.

Reduces cost through code reuse and greater scalability of applications.

Enhances data value by promoting reuse, thereby avoiding bad data.

Implications

Provide proper application program interfaces (APIs) to the data.

Require a common, reusable data access method that promotes interoperability.

Standardize data definitions and business rules.

Design and develop applications in compliance with federal legislation and policies to assure appropriate information availability, sharing, integrity, and utility.

Document applications at all levels of the system lifecycle and store in a repository and include version control.

Optimize application performance for the environment in which the application will run.

Analyze business functions from an enterprise perspective.

Create and maintain an active data dictionary.

17 Electronic Records Capture

17.1 Records Mgmt

All vital records will be captured electronically and managed with the agency's COOP.

Rationale

Ensures ready access to vital records

18 Ensure Security, Confidentiality and Privacy

18.1 Infrastructure

Network systems must be designed and implemented in accordance with security and privacy legislation & policies to assure information confidentiality, integrity and availability.

Rationale

Complies with the Computer Security Act, the Privacy Act of 1974, and Office of Management and Budget (OMB) Circular A-130 “Management of Federal Information

Enhances the integrity of the information.

Enhances the proper stewardship over information.

Enhances public trust.

Helps safeguard confidential and proprietary information.

Implications

Network security is a major part of the network management service and needs to be “resourced’ appropriately.

Need for recognition that interoperability and security may be impossible between vendor products that adhere to “standards for interoperability” (e.g., if using virtual private networks (VPN) directly from firewalls, the current major firewall vendors don’t interoperate although both ostensibly support interoperability).

Network security needs to be integrated with security programs.

Network security must be “baked in and not painted on.”

Network security has major impact on network operations and increases the complexity of troubleshooting (e.g., tracing, Internet Control Message Protocol (ICMP)).

18.2 Security

IT systems should be designed and implemented in accordance with security and privacy legislation and policies to assure information confidentiality, integrity and availability.

Rationale

Enhances the proper stewardship over information.

Enhances public trust.

Complies with the Federal Information Security Management Act (FISMA).

Complies with the Computer Security Act, the Privacy Act of 1974, and OMB Circular A-130 “Management of Federal Information Resources” and the generally accepted principles and practices of IT security.

Enhances the confidentiality, integrity and availability of the information.

Helps safeguard confidential and proprietary information.

Implications

Security must be included in the IT planning and budgeting processes.

System security certification and accreditation must be done prior to placing the system into operation and re-certified/ re-accredited periodically.

Need to identify, publish and keep the applicable policies, procedures and attendant interpretations thereof.

Need for education on issues of privacy, security, and confidentiality to become routine part of normal business processes.

Security has to be integral part of systems life cycle management (e.g., “baked in, not painted on”).

Accountability, enforcement, and compliance mechanisms need to be created/ expanded (e.g., after-the-fact audits cannot replace good security based mechanisms).

Criteria used for classifying information/data needs to be flexible to accommodate changes in the threat environment (e.g., Homeland security).

Need to make the security, confidentiality and privacy requirements clear to designers,

developers, users, system owners and operations personnel.

19 Ensure Security, Integrity, Confidentiality and Privacy

19.1 Application Development

IT systems should be designed and implemented in accordance with security, integrity, confidentiality and privacy legislation and policies to assure appropriate information availability.

Rationale

Helps safeguard confidential and proprietary information.

Enhances public trust.

Enhances the proper stewardship over information.

Enhances the integrity of the information.

Complies with the Computer Security Act, the Privacy Act of 1974, and OMB Circular A-130 “Management of Federal Information Resources.”

Implications

Identify, publish and keep the applicable policies and attendant interpretations current.

Interior may need to develop classification schemes for information security.

Train designers, developers, analysts and operational personnel so they understand security, confidentiality and privacy requirements.

20 Enterprise Management

20.1 Records Mgmt

Electronic records management systems (ERMS) and electronic document management systems (EDMS) will be managed on an enterprise-wide basis.

Rationale

Interoperability is enhanced.

Independent solutions are costly and redundant

21 Enterprise Network as “Virtual” LAN

21.1 GIS

We must implement an Interior-wide “interoperable network”; performing as if it were a virtual, Interior-wide Local Area Network (LAN).

Rationale

Networks are the essential enabling technology for client/server, Internet, and collaborative computing (e.g., emails, file transfers (e.g., file transfer protocol (FTP)), secure teleconferencing, workflow, geospatial data).

Lack of a robust network architecture will impact the success of distributed applications.

Knowledge workers have increasing need for access to information across Interior; this access must appear seamless.

Expands the vision of organizations by reaching out to customers and suppliers.

Implications

Need to implement a robust, interoperable directory services capability.

Requires higher speed and higher bandwidth networks.

Need to create connections between legacy systems, client/server and Internet

Need to define guidelines around “who pays”, “who uses”, “who gets”, and “who coordinates” these interoperable networks.

Policies and protocols on sharing and exchanging information with third parties need to be addressed (e.g., restricted sub-nets will need to be supported).

Need to accommodate remote locations with limited communications options.

Will need the interconnection of distributed LANs.

22 Enterprise Network as a secure "Virtual" Network

22.1 Security

We must implement an Interior-wide "interoperable network" performing as if it were a virtual network.

Rationale

Knowledge workers have an increasing need for secure transmission and access.

External pressures for developing a secure and interoperable network

Implications

Requires secure, remote access gateways, both in and out

Requires higher speed and higher bandwidth networks.

Requires elimination of all "back-door" access to networks

Requires effective and coordinated perimeter security.

Need to implement a robust, interoperable directory services capability.

Need to continue developing our VPN capabilities to allow secure remote access

Will need the interconnection of distributed Local Area Networks (LANs).

Need to create secure connections between legacy systems, client/server and Internet applications.

Policies and protocols on sharing and exchanging information with third parties need to be addressed (e.g., restricted sub-nets will need to be supported).

Need to accommodate remote locations with secure communication options.

Intra-bureau networks will have to develop "trust mechanisms."

Need to identify the perimeter of the network.

Need to define guidelines around "who pays", "who uses", "who gets", and "who coordinates" these interoperable networks.

23 Individual Security Responsibility

23.1 Security

All Interior employees, contractors, partners, etc. share responsibility for Interior's IT Security.

Rationale

Responsibility for security must be shared because IT cannot do it alone.

Required by federal laws and regulations.

Supports the generally accepted principles and practices of IT security.

Implications

Systems owners must take a proactive role in securing their systems. They need to work with managers to ensure that employees working on those systems get appropriate training and adequate time to perform.

All management levels must ensure that adequate resources are provided for security and its appropriate priority.

Accountability and personal liability must be clearly communicated.

Non-security professionals need to be made aware of security policies, procedures and their responsibilities.

24 Industry Proven/ State-of-the-Art Technologies

24.1 Application Development

IT solutions will use industry-proven and "state-of-the-art" technologies.

Rationale

Avoids dependence on weak vendors.

Enables greater use of commercial-off-the-shelf solutions.

Ensures robust product support.

Complies with OMB Circular A-130 "Management of Federal Information Resources", which requires the application of up-to-date information technology to take advantage of opportunities to promote fundamental changes in agency structures, work processes, and ways of interacting with the public that improve the effectiveness and efficiency of Federal agencies.

Implications

With the use of proven technologies, we may be slower to adopt the latest technologies.

Need resources to adequately manage the life cycle of all application acquisition and development technologies including the incorporation of new technologies.

"State-of-the-art" implies a much higher added level of service to customers.

Requires the technology portfolio to migrate away from existing weak products or products that are reaching obsolescence.

The exploration of new technology should be encouraged and the findings shared across the department.

"Industry proven" may include solutions that are not from recognized vendors and/or encompass "freeware" (e.g., Apache servers).

Need to establish the criteria to identify the strongest technology solutions.

25 Industry Standards

25.1 GIS

Extra value will be given to products adhering to industry standards and open architecture.

Rationale

Enables greater use of commercial-off-the-shelf solutions.

Allows flexibility and adaptability in product enhancement, extensibility, and

Reduces dependence on single vendor.

Reduces risks.

Required to support data and process interoperability.

Implications

Participation in the development of open standards is mandatory.

Public open standards will need to be used for distribution of geospatial data to "outside" participants (e.g., public) to avoid proprietary formats.

Need effective management process to identify and assess industry standards and share standards information across Interior.

Need for Interior-wide core standards for exchanging geospatial data among bureaus.

Training and education are required to promote the use of "open standards."

26 Industry Standards and Open Architecture

26.1 Application Development

Application development should adhere to industry standards and open architecture.

Rationale

Lengthens the life of applications and reduces overall cost.

Lessens the chance that applications become technically obsolete.

Systems are more likely to be interoperable.

Allows flexibility and adaptability in product enhancement, extensibility, and

Reduces dependency on a single vendor; i.e., vendor lock-in.

Implications

Promote participation in the development of open standards.

Provide training and education to promote the use of open standards.

Establish and maintain a mechanism to coordinate Interior participation in standards

Develop an effective management process to identify and assess industry standards and share information across Interior.

27 Information Access

27.1 Application Development

Applications must be developed to provide easy and timely access to data and information without security and privacy being compromised.

Rationale

Productivity, decision-making, and customer service are benefits from easy, direct, and timely availability of information.

Develop, acquire and use information technology that is accessible to individuals with disabilities in accordance with the Rehabilitation Act of 1998.

Enable information to be attainable in the appropriate place, time, format and context.

Make records that are frequently requested under the FOIA available for public inspection. Further, records created on or after November 1, 1996 must be available via the Internet or other electronic means.

Incorporate privacy protections required by the Government Paperwork Elimination Act when developing electronic processes.

Beyond the legal requirements, easy and timely access to data and information makes sound business sense.

Provide employees and the public with efficient, effective, and economical access to Government information in accordance with the Paperwork Reduction Act (PRA, PL 104-

Implications

Make information available in formats accessible to those with sensory disabilities in accordance with Section 508.

Provide a variety of public and private access methods for public information in accordance with E-FOIA.

Do not permit sensitive information to be accidentally released.

Clearly state the classification of information and define the classification rules well.

Clearly state the designation of data sensitivity.

Present data in compliance with applicable data access statutes, regulations, business, legal mandates, and public policy.

Presumes the right to know for unclassified information unless policy or law specify otherwise; however, for information like “pre-decisional information”, access would still

Establish the business necessity of sharing information.

Deploy technology to distribute and allow access to information.

27.2 Distributed Systems Management

Ensure that information is stored so that it is accessible for short and long term needs.

Rationale

Enable data and disaster recovery.

Ensures access to current information in a format that is useful internally and

Enables data reuse.

Provides capacity and growth planning metrics.

Implications

Software must be distributed that enables stewards to provide their data to users.

Need to maintain a controlled information storage environment.

Need to ensure that storage products are industry standard and included as part of the data or information when retired; need to identify storage media and hardware that has a significant expected longevity.

Need to follow departmental records management policies and procedures.

Need replication technology as appropriate for the information.

Will require proper capacity planning, performance monitoring, network, LANand LAN/systems tools.

27.3 GIS

Easy and timely access to data and information is the rule rather than the exception without security, confidentiality, and privacy being compromised.

Rationale

The Rehabilitation Act of 1998 requires executive agencies to develop, acquire and use information technology that is accessible to individuals with disabilities.

Productivity, decision-making, and customer service all benefit from easy, direct, and timely availability of information.

The Government Paperwork Elimination Act (GPEA) requires agencies to incorporate privacy protections when developing electronic processes.

In accordance with the Paperwork Reduction Act (PRA, PL 104-13), employees and the public should have efficient, effective, and economical access to Government

Information should be attainable in the appropriate place, time, format and context.

Beyond the legal requirements, easy and timely access to data and information makes sound business sense.

Under Electronic Freedom of Information Act (E-FOIA) bureaus and offices are required to make records that are frequently requested under the FOIA available for public inspection. Further, records created on or after November 1, 1996 must be available via the Internet or other electronic means.

Implications

Technology must be deployed to distribute and allow access to information.

Need to identify, publish and keep the applicable policies and attendant interpretations

The business necessity of sharing information must be established.

For unclassified information, the right to know should be presumed unless policy or law specify otherwise; however, for information like “pre-decisional information”, access would still be controlled.

Sensitive information must not be accidentally released (e.g., copyright).

A variety of public and private access methods for public information in accordance with E-FOIA will need to be provided.

Classification and sensitivity of information must be clearly stated and the rules well defined (e.g., locational precision protected where an archeologically significant site or a nuclear power plant is located).

Every attempt will be made to make information available in formats accessible to those with sensory disabilities in accordance with Section 508 without incurring an undue

27.4 Infrastructure

Easy and timely access to data and information is the rule rather than the exception without security and privacy being compromised.

Rationale

Beyond the legal requirements, easy and timely access to data and information makes sound business sense.

The Government Paperwork Elimination Act (GPEA) requires agencies to incorporate privacy protections when developing electronic processes.

Under Electronic Freedom of Information Act (E-FOIA) bureaus and offices are required to make records that are frequently requested under the FOIA available for public inspection. Further, records created on or after November 1, 1996 must be available via the Internet or other electronic means.

Productivity, decision-making, and customer service all benefit from easy, direct, and timely availability of information.

The Rehabilitation Act of 1998 requires executive agencies to develop, acquire and use information technology that is accessible to individuals with disabilities.

Information should be attainable in the appropriate place, time, format and context.

In accordance with the Paperwork Reduction Act (PRA, PL 104-13), employees and the public should have efficient, effective, and economical access to Government

Implications

Easy and timely access (e.g., single sign-on) will increase reliance on WAN reliability.

Need to determine appropriate "service levels" for public and partners (e.g., Rec.gov).

Differentiated service will still be needed (e.g., not every user will require the highest level of network access).

Network impact must be included early in applications planning process (e.g., IDEAS, MAXIMO).

Customers/users will need to provide much more information within a "security profile" for initiating network access (e.g., current network profile, trusted network relationships).

Appropriate levels of redundant (not wasted) network services will need to be

Need a mechanism/ process to resolve conflicts around "appropriate" network security information for the profile.

27.5 Records Mgmt

Easy and timely access to data and information is the rule rather than the exception without security, privacy and confidentiality being compromised.

Rationale

The Rehabilitation Act of 1998 requires executive agencies to develop, acquire and use information technology that is accessible to individuals with disabilities.

Beyond the legal requirements, easy and timely access to data and information makes sound business sense.

Under E-FOIA bureaus and offices are required to make records that are frequently requested under the FOIA available for public inspection. Further, records created on or after November 1, 1996 must be available via the Internet or other electronic means.

Information should be attainable in the appropriate place, time, format and context.

Productivity, decision-making, and customer service all benefit from easy, direct, and timely availability of information.

In accordance with the Paperwork Reduction Act (PRA, PL 104-13), employees and the public should have efficient, effective, and economical access to Government

The Government Paperwork Elimination Act requires agencies to incorporate privacy protections when developing electronic processes.

27.6 Security

Security and privacy must not be compromised in order to accommodate easy and timely access to information.

Rationale

Required by federal laws and regulations

The Government Paperwork Elimination Act (GPEA) requires agencies to incorporate privacy protections when developing electronic processes.

Implications

Data access will be limited to those who "need to know".

Publicly accessible services must be logically isolated from the internal networks to

ensure security.

Effective security may increase the complexity of internal access

By isolating information, public access to information will be easier and more timely.

28 Information is an Interior asset

28.1 Application Development

Information is valued as an Interior asset to accelerate decision-making, improve management, and increase accountability to our stakeholders (e.g., citizens).

Rationale

Information must be shared to maximize effective decision-making across lines of business and with partners.

The value of information is not realized if it is held in isolated pockets.

Increased access leads to improved integrity and relevance of data.

Information is necessary for decision making to support accelerated business process

Information is the foundation of a citizen-centric government.

Implications

Information needs to be structured for easy access and management, timely availability, and use.

Need to recognize that the “visual identity” or “branding” of the Interior-wide web experience itself is an information asset.

To transport and share information, common operational rules are necessary.

Metadata (information about the data, such as source, units of measurement, and collection methods) will need to be developed and made available.

Data warehouses, metadata and data access methods may need to be developed to facilitate information availability.

Supporting policies regarding security, privacy, confidentiality, information sharing, information integrity, utility and data relevance must be developed and implemented.

Need to promote interoperable information management, such as data warehouses and data access methods that facilitate information availability.

28.2 GIS

Information is valued as an Interior asset to accelerate decision-making, improve management, and increase accountability.

Rationale

Information must be shared to maximize effective decision-making across lines of business and with partners.

Information is necessary for decision making to support accelerated business process

Increased access leads to improved integrity and relevance of data.

Supports Office of Management and Budget (OMB) Circulars: A16 “Coordination of Surveying, Mapping and Related Spatial Data Activities”; A-119 “Federal Participation in the Development and Use of Voluntary Standards”; and A-130 “Management of Federal

The value of information is not realized if it is held in isolated pockets.

Supports Executive Order 12906 “Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure”.

Implications

Metadata (information about the data, such as source, units of measurement, and collection methods) will need to be developed and made available.

Data warehouses, metadata and data accesses may need to be developed to facilitate information availability for decision-making.

Information needs to be structured for easy access and management, timely availability, and use.

Need regular training on appropriate use of information and its quality (e.g., refuge vs

legal vs legislative boundaries).

Supporting policies regarding security, privacy, confidentiality, information sharing, information integrity, utility and data relevance must be developed and implemented (e.g., as outlined in FGDC Privacy Act - Newsletter Summer 1998; see: http://www.fgdc.gov/publications/documents/geninfo/fgdcnl798.html).

Need to assure the accuracy and accessibility of the data over time (e.g., mapping historical changes and maintaining it like wetlands).

Need a method for estimating the value of the information assets themselves (e.g., specific Geospatial database is valued at $50M because it would cost that much to

Need to maintain currency of the data and the legacy data itself.

Need to promote interoperable information management, such as data warehouses and data access methods that facilitate information availability for decision-making.

28.3 Records Mgmt

Information is valued as an Interior asset to accelerate decision-making, improve management, and increase accountability.

Rationale

The value of information is not realized if it is held in isolated pockets.

Information is necessary for decision making to support accelerated business process

Information must be shared to maximize effective decision-making across lines of business and with partners.

Increased access leads to improved integrity and relevance of data.

28.4 Security

Information is valued as an Interior asset and must be protected.

Rationale

Unprotected assets lose their value.

Implications

Policies supporting security, privacy, confidentiality, information sharing, information integrity must be developed and implemented.

Procedures for regular estimation of the value of the information assets need to be defined and practiced.

Need to promote secure interoperable information management that facilitates information availability for decision-making.

Data access will be limited to those who “need to know”.

Metadata will need to include a security classification or identification

29 Integration/ Interoperability

29.1 GIS

Systems must be designed, acquired, developed, or enhanced such that data and processes can be effectively shared, for appropriate purposes, across Interior and with our partners.

Rationale

Increased efficiency will better serve our customers (e.g., the public, employees).

Shared data and processes lead to better decision-making and accountability.

OMB Circular A16 “Coordination of Surveying, Mapping and Related Spatial Data

Ensures more accurate information.

Duplication of effort will cause higher support costs.

Implications

Every systems analyst needs to consider enterprise wide impacts when designing enhancing, acquiring or extending the scope or use of applications.

Will need a method for identifying data and processes that need integration, when

integration should take place, the degree of integration versus interoperability, who should have access to the data, and cost justification for integration.

We will need new tools that enable data sharing and the training for their proper use.

Will need common data standards and consistent data management processes across Interior.

Over-integration can lead to difficult data management and inefficient processes.

29.2 Infrastructure

Systems must be designed, acquired, developed, or enhanced such that data and processes can be effectively shared, for appropriate purposes, across Interior and with our partners.

Rationale

Inter-departmental exchange of information requires network interoperability.

Increased efficiency will better serve our customers (e.g., the public, employees, etc.).

Implications

Need for recognition that interoperability and security may be impossible between vendor products that adhere to "standards for interoperability" (e.g., if using VPN's directly from firewalls, the current major firewall vendors don't interoperate although both ostensibly support interoperability.)

Need for Interior-wide working group to provide guidelines on interoperability

Use of common protocols will be necessary

29.3 Records Mgmt

Systems must be designed, acquired, developed, or enhanced such that data and processes can be effectively managed.

Rationale

Ensures more accurate information.

Managed data and processes lead to better decision-making and accountability.

29.4 Security

Security systems must be designed, acquired, developed, or enhanced so that data and processes can be effectively shared, for appropriate purposes, across Interior and with our

Rationale

Increases access to information.

Increased efficiency will better serve our customers (e.g., the public, employees).

Duplicate systems cause higher support costs.

Implications

System security design will migrate to more widely used standards.

When integrating systems, the highest security level of the source systems should be

Every systems analyst needs to consider enterprise wide security impacts when designing enhancing, acquiring or extending the scope or use of applications.

Increased integration/ interoperability will increase risk & security complexity.

Will need common security standards & consistent processes across Interior.

30 Interior-wide interoperable network

30.1 Infrastructure

We must continue to implement an Interior-wide "interoperable network"; performing as if it were a virtual, Interior-wide Network.

Rationale

Lack of robust network architecture will impact the success of distributed applications.

Networks are the essential enabling technology for client/server, Internet, and

collaborative computing (e.g., emails, file transfers, secure teleconferencing, workflow). An interoperable network enables the organization to more easily reach out to customers

E-government users (e.g., public, employees, partners, suppliers) have increasing need for access to information across Interior; this access must appear seamless.

Implications

Operational sharing of information will increase the complexity of network management (e.g., router down in another bureau's sub-network which is not seen at point of customer

Need to increase the coordination among the operations groups (Network Operations Centers (NOC)) (e.g., published and available contact points).

Coordination mechanisms for network security will need to be created (e.g., policies, procedures, processes).

Need to determine appropriate service levels for participants and have capability for variable service levels.

Network will need to be scalable (e.g., unlike DOINet).

Resources to support a "virtual" network will be in addition to current Bureaus network

Coordination across Bureau boundaries for network control will be significant (e.g., DOINet routers were not under bureau control).

Will need the interconnection of distributed LANs.

Need to create connections between legacy systems, client/server and Internet

Requires higher speed and higher bandwidth networks.

Policies and protocols on sharing and exchanging information with third parties need to be addressed (e.g., restricted sub-nets will need to be supported).

Need to accommodate remote locations with limited communications options.

Need to define guidelines around "who pays", "who uses", "who gets", and "who coordinates" these interoperable networks.

Need to implement a robust, interoperable directory services capability.

31 Mainstream Technologies

31.1 Data Management

Data management will use industry-proven and mainstream technologies.

Rationale

Enables faster deployment of systems.

Complies with OMB Circular A-130 "Management of Information Resources", which requires the application of up-to-date information technology.

Enables greater use of commercial-off-the-shelf solutions.

Promotes robust product support.

Increases the probability that solutions remain viable through the system lifecycle.

Implications

Need a coordinated mechanism for sharing information on industry-proven, mainstream technologies.

Need criteria and an on-going process to assess vendors and products.

Requires the maintenance of data management technology information in the Technical Reference Model/Standards Profile.

31.2 GIS

IT solutions will use industry-proven and "state-of-the-art" mainstream technologies.

Rationale

Ensures robust product support.

Enables greater use of commercial-off-the-shelf solutions.

Avoids dependence on weak vendors.

Complies with OMB Circular A-130 “Management of Federal Information Resources”, which requires the application of up-to-date information technology to take advantage of opportunities to promote fundamental changes in agency structures, work processes, and ways of interacting with the public that improve the effectiveness and efficiency of Federal agencies.

Implications

We may be slow to adopt new technologies.

Need to establish the criteria to identify the weak vendors and poor technology solutions in compliance with Federal government contracting policy and procedures.

Conversions may result in explicit loss of data (e.g., Michigan project with 2-5% of the data content was lost due to a format change).

Requires the technology portfolio to migrate away from existing weak products or products that are reaching obsolescence.

Changing from mainstream vendor’s products within Geospatial technologies will incur significant conversion costs (e.g., maintenance of existing geospatial legacy data) and loss of support for our partners (e.g., other agencies, customers).

The exploration of new technology will be managed and investigation results shared.

Need to establish criteria for vendor selection and performance measurement.

31.3 Infrastructure

IT solutions will use industry-proven and “state-of-the-art” mainstream technologies.

Rationale

Ensures robust product support.

Enables greater use of commercial-off-the-shelf solutions.

Complies with OMB Circular A-130 “Management of Federal Information Resources”, which requires the application of up-to-date information technology to take advantage of opportunities to promote fundamental changes in agency structures, work processes, and ways of interacting with the public that improve the effectiveness and efficiency of Federal agencies.

Avoids dependence on weak vendors.

Implications

Analysis of network solutions will need to be more thorough (e.g., is capability mainstream or vendor?).

Need to use simplified or pre-existing contracts (e.g., National Aeronautics and Space Administration Scientific and Engineering Workstation Procurement III (NASA SEWPIII), 8(a)) to expedite the procurement process when using network mainstream solutions (e.g., rapid changes in underlying technologies).

Need to establish the criteria to identify the weak vendors and poor technology solutions in compliance with Federal government contracting policy and procedures.

We may be slow to adopt new technologies.

The exploration of new network technology will be managed and investigation results

When considering support for mainstream technologies, there will be need to appropriately differentiate bundled versus unbundled solutions (e.g., Microsoft’s Smart

Requires the technology portfolio to migrate away from existing weak products or products that are reaching obsolescence.

Vendor implementations of mainstream network standards many not be compatible (e.g., IP Secure (IPSEC)).

32 Maintain Network Interoperability

32.1 Distributed Systems Management

Use networks management, systems management and performance monitoring tools to maintain the interoperability of the network.

Rationale

Enable near-real-time fault identification.

Enhances sharing of data and information.

Implications

Enables optimization of IT resources.

Will drive Interior to standardized network architectures.

Requires changes to the network environment (money and resources).

33 Network Planning

33.1 Infrastructure

For cost effective network planning, the voice and data planning groups must work together.

Rationale

Network costs will be lower.

Voice and data networks are becoming interchangeable (e.g., convergence).

Implications

Education of local network personnel (voice and/or data) on tradeoff potentials.

Need for rudimentary models of network costing and network architecture for planning during system development process (e.g., for boundary estimations).

May need to provide incentives for coordinating between local voice and data network personnel.

Data network planners need input from local voice planners.

Analysis & decision processes for local service may need to include input from data network organization.

Need modified (new) system development process to explicitly identify the network impacts to the total costs early in the design stage.

34 Personnel security

34.1 Security

All employees, vendors, business partners, consultants and contractors who require access to business information must be appropriately screened, trained and monitored.

Rationale

Ensures a baseline of security awareness.

Required by federal laws and regulations

Helps lower the overall risk, since you are only as secure as your weakest link.

Supports the generally accepted principles and practices of IT security.

Implications

Contracts/ negotiations with unions will need to be modified (e.g., change in working conditions).

Accountability and personal liability must be clearly communicated.

Need to acquire/develop forensic capabilities (e.g., chain of custody, evidence

Appropriate use/acceptable use needs to be clearly defined and regularly communicated.

Need to have a damage assessment capability (e.g., “how big was information hole created by backhoe?”).

Need periodic training and a mechanism (e.g., records management system) to track that it has been done.

Position descriptions and performance standards will need to be revised.

Contracts for non-feds will need to include security responsibilities.

Need to have an enforcement mechanism.

Need to ensure consistency across and among bureaus.

Need to develop guidelines for actions to take when someone violates security policy.

35 Product Standards

35.1 Security

Extra value will be given to security products and/or components adhering to federal standards and non-proprietary open architecture.

Rationale

Required to support adequate levels of security.

Implications

1. Need effective management process to identify and assess federal security standards, guidelines, laws and regulations.

3. Training and education are required to promote the use of “open standards.”

2. Participation in the development of open standards is desirable; otherwise, someone else will do it for you (e.g., litigation.)

36 Provide Reliable Metrics

36.1 Distributed Systems Management

Select appropriate tools to provide reliable metrics information and reports for proactive distributed systems management.

Rationale

Creates reliable metrics and reports to measure success, provide feedback and enable future planning.

Implications

Need to overcome resistance to having machines touched by monitoring tools; need management buy-in.

Need to develop and follow an appropriate use policy for using measurement tools.

Need to understand and follow the laws and regulations governing monitoring.

Need to ensure that the “overhead” of management tools areis not too intrusive so that it outweighs the value they provide.

Need to develop metrics definitions and select tools that support those definitions.

Need appropriate training for tools to understand and utilize full capabilities.

37 Radio Operations

37.1 Infrastructure

Radio operations will adhere to National Telecommunications and Information Administration (NTIA) regulations (e.g., Electronics Industry Association/Telecommunications Industry Association 102 (EIA/TIA 102)).

Rationale

Need for interoperability among bureaus and external partners

Mandated by narrow banding directives from Federal Communications Commission (FCC), NTIA and Interior.

Implications

Need for research effort to explore future capabilities using this technology (e.g., linking Land Mobile Radios (LMR) over data networks).

Need streamlined frequency management capabilities (e.g., memorandum of agreement (MOA)) within department and with external partners (e.g., states).

Additional training will be needed for users (e.g., reprogramming radios).

Need over the air re-keying (OTAR) capabilities to be implemented.

Existing analog systems will need to be replaced.

Need for closer coordination between radio and data network organizations.

Need coordination of operational standards across federal agencies.

Need participation on Project 25 standards and user groups.

Need for wide spread support and maintenance (e.g., vendor).

Need over the air programming (OTAP) capabilities to be implemented.

38 Reengineer First

38.1 Application Development

Business processes will be analyzed, simplified or otherwise redesigned in preparation for and during systems enhancements, development, and implementation.

Rationale

Enables E-Government initiatives.

Provides better customer service.

Required by Clinger-Cohen Act and OMB Circular A-130 "Management of Federal Information Resources" before an IT investment can be made, and promotes compliance with the Government Performance and Results Act (GPRA).

Internet has become a common utility and the public expects government to provide information and access using this utility.

Work processes, activities, and associated business rules will be well understood and documented.

Work processes should be streamlined, efficient, and cost-effective.

Potentially reduces the total cost of ownership.

Implications

May result in new ways of relating/ linking our information.

May result in additional new process modifications and systems development being initiated not long after the completion of a reengineered process that includes the Web.

Organizational change may be required to implement reengineered business processes.

Business processes must be optimized to align with business drivers.

Need agreed upon business process re-engineering scope and results to enable continual improvement through analyzing, simplifying and redesigning work processes.

New technical capabilities will need to be considered in conjunction with normal review of business processes.

Need thorough understanding and documentation of current existing business processes.

Additional time and resources will have to be invested in business analysis early in the systems life cycle.

Requires all organizational levels, especially senior leadership to sponsor and support reengineering efforts.

38.2 GIS

Business processes will be analyzed, simplified or otherwise redesigned in preparation for and during information systems enhancements, development, and implementation.

Rationale

Work processes, activities, and associated business rules will be well understood and documented.

Required by Clinger-Cohen and OMB Circular A-130 "Management of Federal Information Resources" before an IT investment can be made, and promotes compliance with the Government Performance and Results Act (GPRA).

Potentially reduces the total cost of ownership.

Provides better customer service.

Work processes will be streamlined, efficient, and cost-effective.

Enables E-Government initiatives.

Implications

Need system sponsors to include the impact of geospatial data on their goals.

Need for system owners and developers to understand that visualization can be used as a starting point for initial systems analysis and understanding complex processes.

Cultural change may be required to implement reengineered business processes that include geospatial technologies.

Additional time and resources will have to be invested in business analysis early in the systems life cycle.

New technology will need to be researched and applied in conjunction with business process review (e.g., don't use "new" just because it's new).

Need training for developers (both Geospatial and Non-Geospatial knowledgeable) on using geospatial information.

Requires all organizational levels, especially senior leadership to sponsor and support reengineering efforts.

Need agreed upon business process re-engineering scope and results to enable continual improvement through analyzing, simplifying and redesigning work processes.

39 Requirements Definition

39.1 Application Development

Requirements must be thoroughly defined to determine whether it is best to reuse, buy COTS/GOTS or build an application system.

Rationale

Choosing the right approach, based on clearly defined requirements, can save time and cost over the lifecycle of the application system.

Implications

Good system specifications will be needed early in the planning cycle to evaluate

Consider technology trends and technology market direction.

Involve all stakeholders in the definition of systems requirements.

Identify and maintain "reusable" components.

Take the entire application architecture into consideration during the selection process.

Do not select technical solutions before fully understanding functional and technical requirements.

Select application tools that satisfy requirements; do not select tools solely based on current skills.

Balance the costs of providing interoperability and customization as part of the total cost of ownership in selecting application solutions.

40 Reuse before you buy and buy before you build

40.1 GIS

In considering system requirements (e.g., new functionality), we should look to reuse existing components before we buy. If no components exist, purchased solutions (e.g., commercial-off-the-shelf (COTS) or government-off-the-shelf (GOTS)) should be explored before we build.

Rationale

The more you're "like" everyone else (e.g., same standard, same systems), the easier it is to share with others.

Supports Executive Order 12906 "Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure".

Complies with, the Privacy Act of 1974 and the Government Information Systems Reform Act (GISRA).

System development is not a primary mission of Interior.

Supports Office of Management and Budget (OMB) Circulars: A16 "Coordination of Surveying, Mapping and Related Spatial Data Activities"; A-119 "Federal Participation in

the Development and Use of Voluntary Standards"; and A-130 "Management of Federal

Implications

Business processes may need to be "changed" but not compromised to ensure compliance with Interior and Federal standards, to accommodate reuse or purchased

When acquiring data from private vendors, licensing restrictions should be considered.

Need to define, identify and maintain "reusable" components.

System design will migrate to "open" standards.

Requirement for greater sensitivity to the possibility of losing mission responsibility when using outside resources.

In-depth knowledge of system functions may be outside of the organization, potentially increasing issues of risk and cost. Therefore, it will require the metadata information like the process, references (e.g., algorithms), and documentation (e.g., 50% of programming code is remarks) as well as acquiring the digitally delivered unencrypted original source code from the software vendor.

Good system specifications will be needed early in the planning cycle to evaluate

40.2 Records Mgmt

In considering system requirements (e.g., new functionality), we should look to reuse existing components before we buy. If no components exist, purchased solutions (e.g., COTS or GOTS) should be explored before we build.

Rationale

System development is not a primary mission of Interior.

The more you're "like" everyone else (e.g., same standard, same systems), the easier it is to share with others.

Complies with OMB Circular A-130, the Privacy Act of 1974, the Government Information Systems Reform Act, and National Archives and Records Administration

40.3 Security

In considering system security requirements (e.g., new functionality), we should look to reuse existing components before we buy. If no components exist, purchased solutions (e.g., COTS or GOTS) should be explored before we build.

Rationale

The more you're "like" everyone else (e.g., same standard, same systems), the easier it is to share with others.

Complies with Office of Management and Budget (OMB) Circular A-130 "Management of Federal Information Resources", the Privacy Act of 1974, and the Federal Information Security Act (FISMA) of 2003.

Implications

In-depth knowledge of security functions may be outside of the organization, potentially increasing issues of risk and cost.

System security design will migrate to more widely used standards.

Need to identify and maintain "reusable" components.

Good system security specifications will be needed early in the planning cycle to evaluate alternatives.

Business processes may need to be "changed" but not compromised to ensure compliance with Interior and Federal security standards, to accommodate reuse or

41 Reuse Technology Components

41.1 Distributed Systems Management

Use distributed systems management tools to determine the availability and appropriateness of reusable technology components.

Rationale

Enables proactive planning.

Helps inform reuse, buy, or build decisions.

Allows redistribution of resources.

Implications

Need a formal mechanism to proactively promote technology reuse opportunities.

Enables the appropriate allocation of budget dollars.

Need to dedicate resources to actively monitor systems performance and assets.

Need to establish and maintain a baseline.

42 Security, Privacy and Confidentiality

42.1 Records Mgmt

IT systems should be designed and implemented in accordance with security, confidentiality and privacy legislation and policies to assure appropriate information availability.

Rationale

Enhances public trust.

Complies with the Computer Security Act, the Privacy Act of 1974, and OMB Circular A-

Helps safeguard confidential and proprietary information.

Enhances the integrity of the information.

Enhances the proper stewardship over information.

43 Spatial components

43.1 GIS

Most data within Interior has a Geospatial component; our databases must reflect that fact.

Rationale

Geospatial information adds significant value to data.

Geospatial technology is the information and analytical tool for geographic enterprises.

Interior is a geographically based organization.

Better communications and decision-making can be made through the visualization of complex information.

Implications

Applications must not remove geospatial references during processing.

Need for Geospatial reference review during system development process.

Adding Geospatial components to legacy data may be expensive.

Need training for developers (both Geospatial and non- Geospatial knowledgeable) on using geospatial information.

Need common business model for relational database (e.g., keys, data content,

44 Support Business Continuity

44.1 Distributed Systems Management

Use distributed systems management tools to support business continuity planning and operations.

Rationale

Allows the Interior to better recognize failure by establishing baselines and monitoring the IT infrastructure.

Enables future planning.

Enhances public trust.

Reduces the downtime resulting from failures.

Enables assessment and development of continuity of operations and disaster recovery plans; thereby, enabling better ability to recover from a disaster.

Contributes to capturing total cost of ownership information and utilization.

Supports compliance with Office of Management and Budget (OMB) A-130, "Management of Federal Information Resources."

Implications

Need to develop an understanding of cost/risk relationship; costs will increase to mitigate the risk of disaster.

Better baseline information enables better planning and decision-making.

Need an agreed upon process/approach to conducting and maintaining the baseline.

Need identified owners responsible for establishing and maintaining the baseline.

Requires a cultural change for IT staff to report changes in the IT environment.

45 Support Security, Privacy and Confidentiality

45.1 Distributed Systems Management

Select distributed systems management tools that are aligned with security, privacy and confidentiality legislation and policies.

Rationale

Reduces the likelihood of divulging employee and customer privacy information or sensitive systems information.

Enhances public trust.

Enhances Interior's security posture.

Reduces Interior's legal risk.

Implications

DSM tools and IT staff need to have a high level of authority to function; therefore, the IT staff needs higher security awareness and accountability.

Need to be aware of unintended consequences (i.e., using certain tools increases the risk of exposing sensitive information).

IT staff needs appropriate training on DSM tools; users and managers need to be informed about the purpose, appropriate use, functionality, capabilities and limitations of

Need to know which security, privacy and confidentiality legislation and policies are in

DSM tool usage needs to be limited to the appropriate operational levels.

46 System Life Cycle

46.1 Application Development

Use industry standard Systems Life Cycle processes to accommodate multiple methodologies and technologies.

Rationale

Increases the likelihood that stakeholders will deem an application a success.

Reduces costs by creating a common set of repeatable processes.

Leads to a common set of documentation that facilitates reuse, maintenance and reengineering.

Spells out best practices.

Reduces maintenance and reprogramming costs over the long term.

Provides a flexible framework for application development.

Implications

SDLC includes traceability of requirements from business requirements to technical specifications to test cases.

Provide SDLC Methodology training and education.

May extend the initial phases of software development lifecycle, although the overall SDLC may be shorter.

Understand the relationship between SDLC process and outputs and the full system

Choose the appropriate methodology for the scope of the system.

47 The Network is an Interior asset

47.1 Infrastructure

The Network is a valued asset of Interior and must be managed.

Rationale

Information must be shared to maximize effective decision-making and the network is the transport for sharing.

Implications

Need for improved cross-bureau network coordination (e.g., Interior Network Council).

Network impact must be included early in applications planning process (e.g., Interior Department Electronic Acquisition System (IDEAS), MAXIMO).

Continuity of Operations Planning (COOP) needs to include impacts on Interior's network resources.

Valuation of the network asset needs to be addressed (e.g., replacement costs, maintenance costs, equitable charge back).

As with any asset it requires regular depreciation/ replacement costs and understanding by the management and user communities.

Need to develop a model to understand impacts of network "outages" to customer service levels.

Network capacity planning tools will be needed and used across Interior.

Need for periodic review with users to assure network is aligned with business directions.

48 Total Cost of Ownership

48.1 Application Development

Interior will adopt a total cost of ownership (TCO) model.

Rationale

Enables improved planning and budget decision-making.

Leads to better-informed decisions through an improved understanding of trade offs.

Implications

Need for the TCO model to include all affected stakeholders (to address their buy-in) and that addresses the model's boundaries (e.g., Bureau, Department).

Need to develop a total cost of ownership model that explicitly includes all software development and acquisition aspects.

48.2 GIS

Interior will adopt a total cost of ownership model (TCO) for IT systems that includes costs like data acquisition and maintenance (e.g., biggest costs of Geospatial elements).

Rationale

Leads to better-informed decisions through an improved understanding of trade offs.

Enables improved planning and budget decision-making.

Implications

Need to apply TCO to portfolio management and records management (e.g., geospatial data sets and hardcopy are part of the data).

Leads to coordinated system replacements, enhancements and retirements.

Need to develop a total cost of ownership model that explicitly includes geospatial data management and educate system sponsors and decision-makers about how to use it.

Geospatial data never really “goes away” so maintenance is high (e.g., 9 track tape of satellite data needs to migrate to new media).

Need for coordinated management to mitigate data maintenance cost (e.g., National Spatial Data Infrastructure (NSDI) framework data sets)

For Geospatial solutions, the data sets have their own life cycle in addition to the software itself (i.e., data is major cost driver with requirements like compliance that add

Need to provide tools for collection of the actual total cost of ownership.

48.3 Infrastructure

Interior will adopt a total cost of ownership model for IT systems that includes life-cycle considerations such as the costs of development, implementation/transition, support, disaster recovery, and retirement as well as the impacts of flexibility, scalability, ease of use and reduction of integration complexity.

Rationale

Enhances the ability to understand a networks costs and to make better and more informed decisions.

Enables improved planning and budget decision-making.

Implications

Need inventory of current network resources and appropriate metrics of measurement.

Cost of “large scale” changes needs to be considered (e.g., AT&T to WorldCom).

Need to coordinate system replacements, enhancements and retirements.

Need to provide tools for collection of the actual total cost of ownership.

Need to develop a total cost of ownership model and educate system sponsors and decision-makers about how to use it.

Need modified (new) system development process to explicitly identify the network impacts to the total costs early in the design stage.

Network system owners must be identified, who are responsible for accurately uncovering the costs and reach of their networks.

Must be able to identify (i.e., estimate) soft costs (e.g., NOC, service levels, personnel requirements).

48.4 Security

Security must be explicitly factored into a Total Cost of Ownership (TCO) model for all IT systems.

Rationale

By including security in the planning process, management commitment will be

Enables improved planning and budget decision-making.

Leads to better-informed decisions through an improved understanding of trade offs that include security

Implications

Need to identify methods to collect security cost portion of TCO.

Need to develop a total cost of ownership model that includes security and educate system sponsors and decision-makers about how to use it.

49 Unified Records Strategy

49.1 Records Mgmt

Electronic records management systems (ERMS) and electronic document management systems (EDMS) will follow a unified department-wide strategy.

Rationale

Independent solutions are costly and redundant

Interoperability is enhanced.

50 Wireless Operations

50.1 Infrastructure

The adoption of wireless devices (e.g., personal digital assistants (PDA's), cell phones, 802.11 devices) must be managed.

Rationale

Uncontrolled implementations can harm/ compromise the network infrastructure.

Implications

For "remote sync" capabilities, a server-based architecture will be needed (e.g., remote sync with server NOT desktop because of potential network security vulnerability).

Costs for network support will increase (e.g., personal computer (PC) & PDA versus PC

Need for limited number of remote sync capabilities (e.g., not all possibilities).

With this area still evolving, the "best of breed" products and standards are not yet

Wireless attachments to any network need proper network security (e.g., VPN).

Need for unified messaging infrastructure (e.g., messages can be delivered to a variety of devices).